# FortiAuthenticator - Release Notes

VERSION 5.4

**FORTINET DOCUMENT LIBRARY**

https://docs.fortinet.com

**FORTINET VIDEO GUIDE**

https://video.fortinet.com

**FORTINET KNOWLEDGE BASE**

http://kb.fortinet.com

**FORTINET BLOG**

https://blog.fortinet.com

**CUSTOMER SERVICE & SUPPORT**

https://support.fortinet.com

http://cookbook.fortinet.com/how-to-work-with-fortinet-support/

**FORTINET COOKBOOK**

http://cookbook.fortinet.com

**FORTINET TRAINING AND CERTIFICATION PROGRAM**

https://www.fortinet.com/support-and-training/training.html

**NSE INSTITUTE**

https://training.fortinet.com/

**FORTIGUARD CENTER**

https://fortiguard.com

**FORTICAST**

http://forticast.fortinet.com

**END USER LICENSE AGREEMENT**

https://www.fortinet.com/doc/legal/EULA.pdf

August 15, 2018

FortiAuthenticator - Release Notes

23-540-507742-20180815

# TABLE OF CONTENTS

# Introduction

This document provides a summary of new features, enhancements, support information, installation instructions, caveats, and resolved and known issues for FortiAuthenticator™ 5.4.0, build 0294.

FortiAuthenticator is a User and identity management solution that provides strong authentication, wireless 802.1X authentication, certificate management, and Fortinet Single Sign-On (FSSO).

For additional documentation, please visit:

http://docs.fortinet.com/fortiauthenticator/

# Special notices

## TFTP boot process

The TFTP boot process erases all current FortiAuthenticator configuration and replaces it with the factory default settings.

## Monitor settings for web-based manager access

Fortinet recommends setting your monitor to a screen resolution of 1600x1200. This allows for all the objects in the web-based manager to be viewed properly without need for scrolling.

## Before any upgrade

Save a copy of your FortiAuthenticator unit configuration prior to upgrading. Go to **System > Dashboard > Status** and select **Backup/Restore > Download backup file** to backup the configuration.

## After any upgrade

If you are using the web-based manager, clear your browser cache prior to login on the FortiAuthenticator to ensure the web-based manager screens are displayed properly.

# What's new in FortiAuthenticator 5.4

Note that this is a patch release. See Resolved issues and Known issues for more information.

For more detailed information, see the FortiAuthenticator 5.4 Administration Guide.

## FortiToken Cloud service

The FortiToken Cloud service now has the following support.

### Cloud-init support for KVM

Support has been added to FortiAuthenticator VM for KVM (OpenStack). Upon first bootup, the config-drive will look for user data (the IP address of port1, the default gateway static route, and DNS servers), and will also looks for meta data used to set the REST API key for the default administrator, set the FortiAuthenticator's FQDN, load the license file, and reboot the FortiAuthenticator.

### New REST API endpoints

New REST API endpoints have been introduced covering FortiGuard messaging, FortiToken Mobile licenses, email servers, user lockout policies, and system information. See the FortiAuthenticator REST API Solution Guide for more information.

## SMS and email two-factor authentication for self-service portal

Self-service portal and guest portal users can provision themselves with either SMS or their email. This feature is useful for lower risk or short-term users.

## Chained authentication

Chained authentication is useful for two-factor authentication where the password validation must be done against a remote LDAP server and OTP validation against a separate remote RADIUS server. Chained authentication OTP validation is conditional on the group membership of the remote LDAP user.

## Password change at first logon

Users are allowed to change their local password on FortiAuthenticator at first logon. This feature prevents administrators from having to call or email the franchisee to deliver user credentials, which is not a secure method of delivery and adds additional time to the onboarding process.

## SCEP renewal private key authenticity check

This feature allows you to enforce that the SCEP renewal request to be signed by the private key of the existing certificate being being renewed.

## Remote RADIUS server timeout

A timeout can be configured between 1-30 seconds (3 by default) for authentication requests to remote RADIUS servers.

## HSTS support

HTTP Strict Transport Security (HSTS) support has been added to avoid SSL sniffing attacks. HSTS instructs browsers to always use HTTPS when accessing a host, even if the original request is for `http://` or unspecified. Set the expiry between 0-730 days (where 0 means no expiry, maximum of two years). The default is set to 180 days.

## User list report extraction

User audit reports can be generated in order to comply with audit requirements.

# Upgrade instructions

Back up your configuration before beginning this procedure. While no data loss should occur if the procedures below are correctly followed, it is recommended a full backup is made before proceeding and the user will be prompted to do so as part of the upgrade process.

For information on how to back up the FortiAuthenticator™ configuration, see the FortiAuthenticator Administration Guide.

## Hardware and VM support

FortiAuthenticator™ 5.4.0 supports:

- FortiAuthenticator 200D
- FortiAuthenticator 200E
- FortiAuthenticator 400C
- FortiAuthenticator 400E
- FortiAuthenticator 1000C
- FortiAuthenticator 1000D
- FortiAuthenticator 2000E
- FortiAuthenticator 3000D
- FortiAuthenticator 3000E
- FortiAuthenticator VM (VMWare, Hyper-V, KVM, and Xen)

## Deprecated hardware models

The following hardware models are EOS and expected to no longer be supported in the upcoming FortiAuthenticator 5.5.0 release:

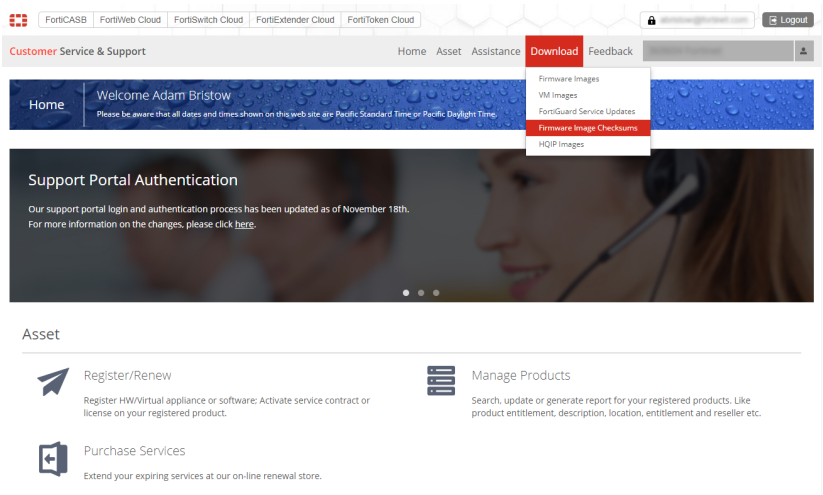
- FortiAuthenticator 3000B

## Image checksums

To verify the integrity of the firmware file, use a checksum tool to compute the firmware file's MD5 checksum. Compare it with the checksum indicated by Fortinet. If the checksums match, the file is intact.

MD5 checksums for software releases are available from the Fortinet Support website.

### Customer service and support image checksum tool




After logging in to the web site, in the menus at the top of the page, click **Download**, then click **Firmware Image Checksums**.

In the **Image File Name** field, enter the firmware image file name including its extension, then click **Get Checksum Code**.

# Upgrading from FortiAuthenticator 4.x/5.0/5.1/5.2

Upgrading the FortiAuthenticator 3000D from 4.0.x to 4.1.x is not supported. The workaround for this model is to upgrade from any 4.0.x version directly to 4.2.0 or higher (skipping all 4.1.x versions).

If you install 4.1.x firmware on a FortiAuthenticator 3000D it stops responding. You can get the system running again by restoring valid firmware using the TFTP boot process.

## Firmware upgrade process

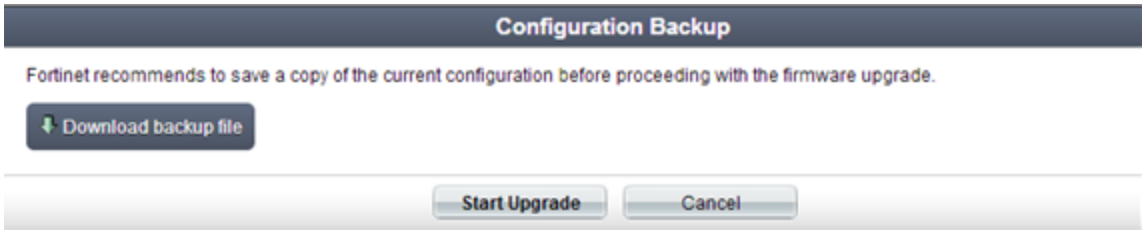
First, back up your configuration, then follow the procedure below to upgrade the firmware.

Before you can install FortiAuthenticator™ firmware, you must download the firmware package from the Fortinet Support website, then upload it from your computer to the FortiAuthenticator™ unit.

1. Log in to the Fortinet Support website. In the **Download** section of the page, select the **Firmware Images** link to download the firmware.
2. To verify the integrity of the download, go back to the **Download** section of the login page and click the **Firmware Image Checksums** link.
3. Log in to the FortiAuthenticator unit's web-based manager using the **admin** administrator account.
4. Go to **System > Dashboard > Status**.
5. In the **System Information** widget, in the **Firmware Version** row, select **Upgrade**. The **Firmware Upgrade or Downgrade** dialog box opens.

6. In the **Firmware** section, select **Choose File**, and locate the upgrade package that you downloaded.
7. Select **OK** to upload the file to the FortiAuthenticator.

Your browser uploads the firmware file. The time required varies by the size of the file and the speed of your network connection. When the file transfer is complete, the following message is shown:




It is recommended that a system backup is taken at this point. Once complete, click **Start Upgrade**.

Wait until the unpacking, upgrade, and reboot process completes (usually 3-5 minutes), then refresh the page.

# Product integration and support

## Web browser support

The following web browsers are supported by FortiAuthenticator™ 5.4.0:

- Microsoft Internet Explorer versions 9 to 11
- Microsoft Edge 42
- Mozilla Firefox versions 61
- Google Chrome versions 68

Other web browsers may function correctly, but are not supported by Fortinet.

## FortiOS support

FortiAuthenticator™ 5.4.0 supports the following FortiOS versions:

- FortiOS v6.0.2
- FortiOS v5.6.5
- FortiOS v5.4.9

The above versions have been verified by QA. Other FortiOS versions may function correctly, but may not be supported by Fortinet. Refer to the What's new in FortiAuthenticator 5.4 section and Known issues for version compatibility information.

## Fortinet agent support

FortiAuthenticator™ 5.4.0 supports the following Fortinet Agents:

- FortiClient v.5.x, v.6.x for Microsoft Windows (Single Sign-On Mobility Agent)
- FortiAuthenticator Agent for Microsoft Windows 2.2
- FortiAuthenticator Agent for Outlook Web Access 1.5
- FSSO DC Agent v.5.x
- FSSO TS Agent v.5.x

Other Agent versions may function correctly, but may not be supported by Fortinet.

For details of which operating systems are supported by each agent, please see the install guides provided with the software.

## Virtualization software support

FortiAuthenticator™ 5.4.0 supports:

- VMware ESXi / ESX 4.0, 4.1, 5.0, 5.1, 5.5, 6.0, and 6.5
- Microsoft Hyper-V 2010, Hyper-V 2012 R2, and Hyper-V 2016
- Linux Kernel-based Virtual Machine (KVM) on Virtual Machine Manager and QEMU 2.5.0
- Xen Virtual Machine (for Xen HVM and AWS)

Support for HA in Active-Passive and Active-Active modes has not been confirmed on the FortiAuthenticator for Xen VM at the time of the release.

See Appendix A: FortiAuthenticator VM for more information.

## Third-party RADIUS authentication

FortiAuthenticator uses standards based RADIUS for authentication and can deliver two-factor authentication via multiple methods for the greatest compatibility:

- RADIUS Challenge Response - Requires support by third party vendor
- Token Passcode Appended - Supports any RADIUS compatible system

FortiAuthenticator should therefore be compatible with any RADIUS capable authentication client / network access server (NAS). For more information, see the FortiAuthenticator Two-Factor Authentication Interoperability Guide.

# Resolved issues

The resolved issues listed below may not list every bug that has been corrected with this release. For inquiries about a particular bug, please visit the Fortinet Support website.

| Bug ID | Description |
|---|---|
| **496055** | SMS token not sent when requested from FortiGate via RADIUS with specific gateway settings. |
| **494702** | Incorrect Content-Type in POST method when SMS token is requested from. |
| **492354** | When STARTTLS is used to send out emails, it fails without sending any traffic. |
| **477632** | Secondary LDAP server is not used for RSSO group resolution. |
| **504812** | RADIUS client's list is not refreshing once a member is deleted. |
| **492539** | Linux Kernel TCP sequence number generation security weakness. |
| **495751** | Remote LDAP password renewal fails via RADIUS. |
| **500679** | FortiAuthenticator does not reliably respect configured FortiGate IP filter. |
| **499949** | Increase tablesize limit for "Remote LDAP Users Sync Rules". |
| **397359** | LDAP connect fail log doesn't display on GUI. |
| **452878** | Incorrect number of revocated certificates in CRLs. |
| **492438** | RADIUS authentications failure with Android phones with MSCHAPV2. |
| **451990** | Warning if FortiClient SSOMA secret key is larger than 15 characters. |
| **501546** | Unable to clone RADIUS client, GUI error. |
| **486544** | FortiAuthenticator fails to connect to AD after cluster failover. |
| **489030** | Disabling user account lockout policy will not disable maximum token code retry limit. |
| **488794** | FortiAuthenticator failed to connect to LDAP server. |
| **493698** | Windows Agent 2.0.2 bypasses two-factor authentication if FQDN name is entered for the user. |
| **289457** | FortiAuthenticator Windows Agent not pre-filling RDP domain in some circumstances. |
| **476697** | Incorrect password, email, and telephone number when importing local users from FortiGate config file. |

| Bug ID | Description |
|---|---|
| **489540** | Attempt to clone a RADIUS client results in GUI error dump. |
| **451555** | User is deactivated if they don't receive an SMS for self-service or guest portal. |
| **463904** | GUI error while re-enabling a user. |
| **444060** | Changes to RADIUS Client IP address are not reflected until the "Save" button in the profile section is selected. |
| **476097** | Can't grant administrator privileges to remote users with spaces in their user name. |
| **496813** | FortiAuthenticator fails to upgrade from 4.3 (b0216) to 5.3 (b0284). |
| **488079** | Guest portal change profile can still be accessed when profile is set to view only. |
| **436030** | SAML IdP signature verification error on logout. |
| **482284** | Upgrade Apache. |
| **491570** | Support dual two-factor authentication for imported local users. |
| **495395** | SSL labs rating degraded due to support for weak DH key exchange parameters. |
| **500932** | Accept pound (#) and apostrophe (') in usernames. |
| **506306** | FortiAuthenticator crashes when attempting to import MAC devices. |
| **503506** | TTLS authentication failure. |
| **489005** | Load-balancing doesn't work until FortiAuthenticator KVM is rebooted. |
| **505914** | Signing in as a different user link is broken for SAML with wrong response input. |
| **499997** | Manually created devices not included in authorized device groups for guest portal device tracking. |
| **504795** | Temporary email tokens not sent to the self-service portal user when token is reported as lost. |
| **504010** | Crash when a regular APAC remote token user login into Guest Portal. |
| **500576** | When a FortiAuthenticator is acting as a RADIUS client, it fails to send a blank response to the challenge request to initiate a push auth. |
| **480885** | SAML authentication for remote RADIUS users causes webserver to crash. |
| **488149** | PCI - Do not allow AD users with expired passwords to change them without token entry. |
| **486923** | Unknown publisher warning when uninstalling FortiAuthenticator Agent. |

| Bug ID | Description |
|---|---|
| **499812** | Token verification fails in guest portal. |
| **483902** | Remote LDAP post login edit profile issue. |
| **498624** | Unable to initiate push notifications via RADIUS requests. |
| **482208** | Integer type no longer supported for "event" field of /ssoauth/ endpoint. |
| **493340** | Load-balanced HA groups with password policy not synchronized. |
| **488042** | Remote LDAP users can't access SAML login portal after promoted to administrator. |
| **481878** | Trying to login to guest portal with a user who doesn't have RADIUS authentication enabled produces unhelpful error message. |
| **493325** | Password reset emails are being sent to users who do not have passwords assigned to them (e.g. FortiToken only authentication). |
| **483921** | Enable Smart Connect without profile. |
| **485559** | Should not allow FortiToken self-revocation actions to proceed if password is invalid (in PCI mode). |
| **492767** | Should not show warning message when HTTP access is not enabled while configuring SCEP. |
| **486190** | Missing administrator profile permissions. |
| **495440** | Uploading license file produces system error. |
| **504194** | FortiAuthenticator models 2000E and 3000E report missing power supply units after being upgraded to 5.3.1. |
| **487387** | Custom fields are not shown in validation request email or GUI. |
| **497106** | FSSO (RADIUS accounting source) with mutliple AD's failing. |

# Known issues

This section lists the known issues of this release, but is not a complete list. For inquires about a particular bug, please visit the Fortinet Support website.

| Bug ID | Description |
|---|---|
| **478985** | FortiAuthenticator Windows Agent sometimes doesn't see the domain name and user is not able to login. |
| **504080** | Possible NTLM thread leak. |
| **503366** | Monitor SSO domains show one DC as red on HA master and green on backup. |
| **501832** | Support RADIUS secrets of up to 64 characters. |
| **482913** | Information from authorityKeyIdentifier is not used to check the correct CRL for revocation status of user certificate. |
| **503150** | FortiAuthenticator syslog SSO matching rule - UnicodeEncodeError on sample data. |
| **507246** | FortiAuthenticator GUI login fails in Chrome and Firefox when two-factor authentication is used and site accessed is via FortiGate SSL VPN web portal. |
| **438383** | CRL HTTP retrieval is not working and documented properly. |
| **461429** | Unexpected guest portal user registration behavior with SMS. |
| **492709** | Downloading create_req.bat from self-service portal leads to error message. |
| **463529** | FortiAuthenticator SAML IdP support for Desktop/Thick O365 clients. |
| **464556** | Time-based user expiry configured in usage profile isn't applied to users when they already have an expiry date configured. |
| **503212** | Device getting disconnections to DC and user authentication issues. |
| **506294** | FortiAuthenticator appears to truncate SSO groups found in long SAML attribute assertions leading to logon failures. |
| **502007** | The RADUIUS accounting and CoA did not take effect in FortiAuthenticator side. |

# Appendix A: FortiAuthenticator VM

## FortiAuthenticator VM system requirements

The following table provides a detailed summary on FortiAuthenticator virtual machine (VM) system requirements. Installing FortiAuthenticator VM requires that you have already installed a supported VM environment. For details, see the FortiAuthenticator VM Install Guide.

**VM requirements**

| Virtual machine | Requirement |
|---|---|
| VM form factor | Open Virtualization Format (OVF) |
| Virtual CPUs supported (minimum / maximum) | 1 / 8 |
| Virtual NICs supported (minimum / maximum) | 1 / 4 |
| Storage support (minimum / maximum) | 60GB / 2TB |
| Memory support (minimum / maximum) | 512 MB / 64GB |
| High Availability (HA) support | Yes |

## FortiAuthenticator VM firmware

Fortinet provides FortiAuthenticator VM firmware images in two formats:

- **.out**
  Use this image for new and upgrades to physical appliance installations. Upgrades to existing virtual machine installations are also distributed in this format.
- **ovf.zip**
  Use this image for new VM installations. It contains a deployable OVF virtual machine package for initial VMware ESXi installations.

For more information see the FortiAuthenticator product datasheet available on the Fortinet web site, https://www.fortinet.com/products/identity-access-management.html#models-specifications.

# Appendix B: Maximum values

This section lists the maximum number of configuration objects per FortiAuthenticator appliance that can be added to the configuration database for different FortiAuthenticator hardware and VM configurations.

The maximum values in this document are the maximum configurable values and are not a commitment of performance.

## Hardware appliances

The following table describes the maximum values set for the various hardware models.

| Feature | | Model | | | | |
|---|---|---|---|---|---|---|
| | | 200E | 400E | 1000D | 2000E | 3000E |
| **System** | | | | | | |
| Network | Static Routes | 50 | 50 | 50 | 50 | 50 |
| Messages | SMTP Servers | 20 | 20 | 20 | 20 | 20 |
| | SMS Gateways | 20 | 20 | 20 | 20 | 20 |
| | SNMP Hosts | 20 | 20 | 20 | 20 | 20 |
| Administration | SYSLOG Servers | 20 | 20 | 20 | 20 | 20 |
| | User Uploaded Images | 30 | 100 | 500 | 1000 | 2000 |
| | Language Files | 50 | 50 | 50 | 50 | 50 |
| **Realms** | | 20 | 80 | 400 | 800 | 1600 |
| **Authentication** | | | | | | |
| General | Auth Clients (NAS) | 166 | 666 | 3333 | 6666 | 13333 |

| Feature | | Model | | | | |
|---|---|---|---|---|---|---|
| | | 200E | 400E | 1000D | 2000E | 3000E |
| | **Users** (Local + Remote)[1] | 500 | 2000 | 10000 | 20000 | 40000 |
| | User Radius Attributes | 1500 | 6000 | 30000 | 60000 | 120000 |
| | User Groups | 50 | 200 | 1000 | 2000 | 4000 |
| | Group Radius Attributes | 150 | 150 | 600 | 6000 | 120000 |
| | FortiTokens | 1000 | 4000 | 20000 | 40000 | 80000 |
| | FortiToken Mobile Licenses[2] | 200 | 200 | 200 | 200 | 200 |
| | LDAP Entries | 1000 | 4000 | 20000 | 40000 | 80000 |
| | Device (MAC-based Auth.) | 50 | 200 | 1000 | 2000 | 4000 |
| | RADIUS Client Profiles | 500 | 2000 | 10000 | 20000 | 40000 |
| | Remote LDAP Servers | 20 | 80 | 400 | 800 | 1600 |
| | Remote LDAP Sync Rule | 25 | 100 | 500 | 1000 | 2000 |
| | Remote LDAP User Radius Attributes | 1500 | 6000 | 30000 | 60000 | 120000 |
| **FSSO & Dynamic Policies** | | | | | | |
| FSSO | FSSO Users | 500 | 2000 | 10000 | 20000 | 200000[3] |
| | FSSO Groups | 1000 | 1000 | 5000 | 10000 | 20000 |
| | Domain Controllers | 10 | 20 | 100 | 200 | 400 |
| | RADIUS Accounting SSO Clients | 166 | 666 | 3333 | 6666 | 13333 |
| | FortiGate Services | 50 | 200 | 1000 | 2000 | 4000 |
| | FortiGate Group Filtering | 250 | 1000 | 5000 | 10000 | 20000 |
| | FSSO Tier Nodes | 5 | 20 | 100 | 200 | 400 |
| | IP Filtering Rules | 250 | 1000 | 5000 | 10000 | 20000 |

| Feature | | Model | | | | |
|---|---|---|---|---|---|---|
| | | 200E | 400E | 1000D | 2000E | 3000E |
| Accounting Proxy | Sources | 500 | 2000 | 10000 | 20000 | 40000 |
| | Destinations | 25 | 100 | 500 | 1000 | 2000 |
| | Rulesets | 25 | 100 | 500 | 1000 | 2000 |
| **Certificates** | | | | | | |
| User Certificates | User Certificates | 2500 | 10000 | 50000 | 100000 | 200000 |
| | Server Certificates | 50 | 200 | 1000 | 2000 | 4000 |
| Certificate Authorities | CA Certificates | 10 | 10 | 50 | 50 | 50 |
| | Trusted CA Certificates | 200 | 200 | 200 | 200 | 200 |
| | Certificate Revocation Lists | 200 | 200 | 200 | 200 | 200 |
| SCEP | Enrollment Requests | 2500 | 10000 | 50000 | 100000 | 200000 |

[1] Note that **Users** is the only metric used for the number of allowed users. **Local Users** and **Remote Users** share the same limit value. This enables **Local Users** *or* **Remote Users** to be equal to **Users** or for there to be a mixture of user types, however, the total number of local and remote users cannot exceed the **Users** metric.

[2] **FortiToken Mobile Licenses** refers to the licenses that can be applied to a FortiAuthenticator, not the number of FortiToken Mobile instances that can be managed. The total number is limited by the FortiToken metric.

[3] For the 3000E, the total number of concurrent SSO users is set to a higher level to cater for large deployments.

## VM appliances

The FortiAuthenticator-VM Appliance is licensed based on the total number of users and licensed on a stacking basis. All installations must start with a FortiAuthenticator VM-Base license and users can be stacked with upgrade licenses in blocks of 100, 1,000, 10,000 and 100,000 users. Due to the dynamic nature of this licensing model, most other metrics are set relative to the number of licensed users. The **Calculating metric** column below shows how the feature size is calculated relative to the number of licensed users for example, on a 100 user FortiAuthenticator-VM Base License, the number of auth clients (NAS devices) that can authenticate to the system is:

**100 / 10 = 10**

Where this relative system is not used e.g. for static routes, the **Calculating metric** is denoted by a "**-**". The supported figures are shown for both the base VM and a 5000 user licensed VM system by way of example.

The following table describes the maximum values set for the various VM models.

| Feature | | Model | | | |
|---|---|---|---|---|---|
| | | Unlicensed VM | Calculating metric | Base VM (100 users) | Example 5000 licensed user VM |
| **System** | | | | | |
| Network | Static Routes | 2 | 50 | 50 | 50 |
| Messaging | SMTP Servers | 2 | 20 | 20 | 20 |
| | SMS Gateways | 2 | 20 | 20 | 20 |
| | SNMP Hosts | 2 | 20 | 20 | 20 |
| Administration | SYSLOG Servers | 2 | 20 | 20 | 20 |
| | User Uploaded Images | 5 | Users / 20 | 5 | 100 |
| | Language Files | 5 | 50 | 50 | 50 |
| **Authentication** | | | | | |
| General | Auth Clients (NAS) | 3 | Users / 3 | 33 | 1666 |
| User Management | **Users** (Local + Remote)[1] | 5 | ********** | 100 | 5000 |
| | User RADIUS Attributes | 15 | Users x 3 | 300 | 15000 |
| | User Groups | 3 | Users / 10 | 10 | 500 |
| | Group RADIUS Attributes | 9 | Users x 3 | 300 | 15000 |
| | FortiTokens | 10 | Users x 2 | 200 | 10000 |
| | FortiToken Mobile Licenses (Stacked) [2] | 3 | 200 | 200 | 200 |
| | LDAP Entries | 20 | Users x 2 | 200 | 10000 |
| | Device (MAC-based Auth.) | 1 | Users / 10 | 10 | 500 |

| Feature | | Model | | | |
|---|---|---|---|---|---|
| | | Unlicensed VM | Calculating metric | Base VM (100 users) | Example 5000 licensed user VM |
| | RADIUS Client Profiles | 3 | Users | 100 | 10000 |
| | Remote LDAP Servers | 4 | Users / 25 | 4 | 200 |
| | Remote LDAP Sync Rule | 1 | Users / 10 | 10 | 500 |
| | Remote LDAP User Radius Attributes | 15 | Users x 3 | 300 | 15000 |
| **FSSO & Dynamic Policies** | | | | | |
| FSSO | FSSO Users | 5 | Users | 100 | 5000 |
| | FSSO Groups | 30 | Users / 2 | 50 | 2500 |
| | Domain Controllers | 3 | Users / 100 (min=10) | 10 | 50 |
| | RADIUS Accounting SSO Clients | 10 | Users | 100 | 5000 |
| | FortiGate Services | 2 | Users / 10 | 10 | 500 |
| | FortiGate Group Filtering | 30 | Users / 2 | 50 | 2500 |
| | FSSO Tier Nodes | 3 | Users /100 (min=5) | 5 | 50 |
| | IP Filtering Rules | 30 | Users / 2 | 50 | 2500 |
| Accounting Proxy | Sources | 3 | Users | 100 | 1000 |
| | Destinations | 3 | Users / 20 | 5 | 250 |
| | Rulesets | 3 | Users / 20 | 5 | 250 |
| **Certificates** | | | | | |
| User Certificates | User Certificates | 5 | Users x 5 | 500 | 25000 |
| | Server Certificates | 2 | Users / 10 | 10 | 500 |

| Feature | | Model | | | |
|---|---|---|---|---|---|
| | | Unlicensed VM | Calculating metric | Base VM (100 users) | Example 5000 licensed user VM |
| Certificate Authorities | CA Certificates | 3 | Users / 20 | 5 | 250 |
| | Trusted CA Certificates | 200 | 200 | 200 | 200 |
| | Certificate Revocation Lists | 5 | 200 | 200 | 200 |
| SCEP | Enrollment Requests | 5 | Users x 5 | 2500 | 10000 |

[1] Note that there is one metric used for the number of allowed users which is **Users**. **Local Users** and **Remote Users** share the same limit value. This enables **Local Users** *or* **Remote Users** to be equal to **Users** or for there to be a mixture of user types, however, the total number of local and remote users cannot exceed the **Users** metric.

[2] **FortiToken Mobile Licenses** refers to the licenses that can be applied to a FortiAuthenticator, not the number of FortiToken Mobile instances that can be managed. The total number is limited by the FortiToken metric.